

## UNITED STATES DISTRICT COURT

for the  
Eastern District of WisconsinU.S. District Court  
Wisconsin Eastern

AUG 2 2023

FILED  
Clerk of Court

In the Matter of the Search of:

Records and information associated with cellular number  
(915) 234-0096, with listed subscriber(s) unknown that is  
stored at premises controlled by **AT&T and all of its  
Subsidiaries and Affiliates**

Case No. 23 M 471

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: which constitutes evidence of Title 18, United States Code, Section 2250(a), Failure to Register as a Sex Offender.

The application is based on these facts: See attached affidavit.

- ☒ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: January 25, 2024, is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature

Samuel Santi, Deputy US Marshal  
 Printed Name and Title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim P. 4.1 by  
TELEPHONE (specify reliable electronic means):

Date: 8/2/2023
  
 Judge's signature
City and State: Green Bay, Wisconsin

JAMES R. SICKEL, U.S. Magistrate Judge  
 Printed Name and Title

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT

I, Deputy U.S. Marshal (DUSMS) Samuel J. Santi, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A), for information about the location of the cellular telephone(s) assigned call number **(915) 234-0096** (the, “Target Cell Phone”), whose service provider is **AT&T and all of its Subsidiaries and Affiliates** (“Service Provider”), a wireless telephone service provider headquartered at 11760 US Highway 1, North Palm Beach, FL 33408. The Target Cell Phone is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen-trap devices”) to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phones.

3. I am presently employed as a Deputy US Marshal (DUSM), with the United States Marshals Service, where I have been employed since June of 2022. I have been a full-time sworn law enforcement officer for 8 months; I have completed approximately 650 hours of instruction at the Federal Law Enforcement Training Center in Glynco, Georgia. I completed blocks of instruction and labs that have enabled me to identify potential sources of electronic evidence,

including but not limited to computers, cell phones, and other digital storage media and to preserve and exploit such evidence. I am currently assigned to the Great Lakes Regional Fugitive Task Force (GLRFTF) and have been so for the past 8 months. As part of my duties as a DUSM, I conduct investigations to locate federal and state fugitives. Many of these investigations were aided by procurement of records related to electronic communications and subsequent analysis of those records. In most of those cases, the records provided critical investigative leads and corroborative evidence. I have had previous experiences using cellular data in order to locate and apprehend fugitives from justice. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations.

4. The facts in this affidavit come from my training and experience, my review of documents and information obtained from other agents, and crucial information from Deputy United States Marshal Rodney Clauss who was the lead investigator prior to his retirement from the United States Marshal Service on July 28, 2023. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that **Jason STACHE** has violated 18 U.S.C. 2250(a) (Failure to Register as a Sex Offender). **STACHE** is the subject of an arrest warrant issued on **September 10, 2021**. There is also probable cause to believe that **STACHE** is aware of these charges and has fled. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting **STACHE**, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

6. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined 18 U.S.C. Section 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. Section 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. The United States government, including the USMS, is conducting a fugitive and criminal investigation of **STACHE** who is currently wanted for violations of Parole through the Wisconsin Department of Corrections (WI DOC), and is under further investigation for violations of Title 18, United States Code, Sections 2250(a)

8. On 5/21/99, **STACHE** was convicted in Brown County, WI, case number 99CF147, of Second Degree Sexual Assault of a Child. On February 15, 2008, **STACHE** was convicted in Brown County case number 07CF804, of Second Degree Sexual Assault of a Child. Based on both convictions, **STACHE** is required to register as a sex offender for life under SORNA and with the Wisconsin Sex Offender Registry (WI SOR). Under Wisconsin law, **STACHE** is required to wear a GPS monitor for life as a Wisconsin resident.

9. **STACHE** last registered with the WI SOR in Green Bay, WI in early September of 2021. On September 10, 2021, **STACHE** cut off his GPS bracelet and absconded. The GPS bracelet was removed in Platteville, WI. On the same date, the WI DOC issued a Parole Violation warrant for **STACHE**. On October 15, 2021, a warrant was issued for **STACHE** out of Grant County, WI, in case number 21CF242 for Tampering with a GPS. **STACHE** has a history of traveling to other states with prior arrests in Oregon, Nevada, California, and Illinois. **STACHE**'s current whereabouts are unknown.

10. In May of 2023, I located a Facebook account for **STACHE**'s mother, Cherice

Lake. On December 13, 2021, Cherice posted a picture on her account. **STACHE** responded to the post using Facebook username “Yesod Dalet”, Facebook ID: 100074963089137.

11. Based upon the information above, Judge Sickel signed a Search Warrant for historical records pertaining to Facebook account <https://www.facebook.com/profile.php?id=100074963089137>. On July 11, 2023, information from the historical records showed that **STACHE** was using the “Yesod Dalet” account. According to the historical records, and confirmed through Facebook, the following phone number was attached to that account: **(915) 234-0096**.

12. On 12/31/21, **STACHE** responded to a picture posted by a Facebook “Friend” by typing: “It’s really too bad you don’t live in Texas or driving distance for (from) me. I run a Modeling Agency. We do nature based and ariel photography for several magazines. Your eyes could pierce threw (through) a soul of stone. Such natural beauty is extremely rare. Contact me, let’s talk. **(915) 234-0096**.”

13. Based on the above information, it is believed that **STACHE** was in possession of (the “Target Cell Phone”) number **(915) 234-0096**. Historical records obtained from the Target Cell phone number will assist law enforcement in locating **STACHE**. Law enforcement databases show the Target Cell Phone number **(915) 234-0096** to be an active wireless cell phone number with **AT&T and all of its Subsidiaries and Affiliates** (the “Service Provider”).

14. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector

records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

15. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

16. Based on my training and experience, I know that the Service Provider also collects per-call measurement data, which the Service Provider also refers to as PCMD. PCMD estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

17. Based on my training and experience, I know each cellular device has one or more

unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication’s content.

18. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers’ use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone user or users and may assist in the identification of co-conspirators and/or victims.

19. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

20. I further request that the Court direct the Service Provider to disclose to the



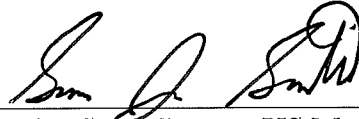
government any information described in Section I of Attachment B that is within its possession, custody, or control.

21. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

22. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

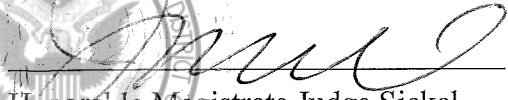


23. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.



Samuel J. Santi, Deputy US Marshal

Subscribed and sworn to me this 2 day of August, 2023.



Honorable Magistrate Judge Sickel

## **ATTACHMENT A**

### **Property to Be Searched**

Records and information associated with the cellular device assigned **(915) 234-0096** (referred to herein and in Attachment B as “the Target Cell Phone”), with listed subscriber(s) unknown that is in the custody or control of **AT&T and all of its Subsidiaries and Affiliates** (referred to herein and in Attachment B as the “Service Provider”), a wireless communications service provider that is headquartered at 11760 US Highway 1, North Palm Beach, FL 33408.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period **9/10/2021–the current date**:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
  - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:
  - (A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - (B) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received) as well as per-call measurement data (also known as “real-time tool” or “RTT”).
- b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:
  - i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
  - ii. Source and destination telephone numbers;
  - iii. Date, time, and duration of communication; and
  - iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as “real-time tool” or “RTT”).
  - v. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of either (i) violations of 18 U.S.C. 2250(a) (Failure to Register as a Sex Offender) involving Jason **STACHE** or (ii) **STACHE**’s flight from justice, since September 10, 2021, including, but not limited to, information pertaining to the following matters:

- (a) **STACHE**’s location; and

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are

authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.